EXHIBIT

1

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF TEXAS DALLAS DIVISION

§	
§	
§	
§	
§	
§	Civil Action No. 3:21-cv-02181-E
§	
§	
§	
§	
	\$ \$ \$ \$ \$ \$

VERA DEFENDANTS' SUPPLEMENT TO THEIR MOTION TO STAY PROVIDING A COPY OF THE SEARCH WARRANT

Defendants, Walter Vera ("Vera"), Verastan Group, LLC ("Verastan") and Midwood Capital, LLC ("Midwood") (collectively the "Vera Defendants"), file their Supplement to their Motion to Stay (Dkt. #313) to include a copy of the Search Warrant they just received on March 5, 2025, which is attached as Exhibit A.

A review of the Search Warrant unquestionably shows the overlap of civil and criminal elements of proof (the facts necessary to prove the Receiver's civil causes of action and the facts necessary to prove criminal liability) is substantial if not identical. As drafted by the FBI, the Search Warrant specifically mentions Walter Vera twice by name as one of the targeted individuals. See Exhibit A, under the heading "II. Search Procedure for Digital Devices," paragraph 8. Additionally, page one of the Search Warrant plainly states the basis for the search

VERA DEFENDANTS' SUPPLEMENT TO THEIR MOTION TO STAY PROVIDING A COPY OF THE SEARCH WARRANT– Page 1

¹ The Magistrate Judge struck through Vera's name in the Search Warrant, presumably for lack of probable cause at the time; but the fact the FBI drafted the Search Warrant with Vera's name typed into it twice shows he is a target of the investigation. Moreover, it is undisputed the FBI seized Vera's personal cell phone during the raid using the Search Warrant.

is "evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing a crime." Exhibit A, p. 1.

Next, the Search Warrant states the search is related to a violation of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1341 (Mail Fraud). Exhibit A, p. 1. When comparing the elements of the Mail and Wire Fraud Statutes to the Receiver's allegations in its First Amended Complaint (the "FAC"), the overlap is obvious. 18 U.S.C. § 1343 states, in pertinent part, as follows:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

18 U.S.C. § 1341 is effectively the same, stating in pertinent part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises . . . places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service . . . shall be fined under this title or imprisoned not more than 20 years, or both.

Thus, the gravamen of the Wire and Mail Fraud statutes is intent to obtain money or property by false or fraudulent means. Here, as shown in the Vera Defendants' Motion to Stay, the Receiver's allegations in the FAC are littered with fraud-based contentions against the Vera Defendants – allegations that, if proven true, would support the basis for Wire and Mail Fraud. For example, the Receiver has alleged in its FAC that the Vera Defendants:

- Received assets from Metals.com (and other Receivership Entities), in exchange for their sale of precious metals and coins, sold at grossly inflated prices based on false and misleading misrepresentations, to unsuspecting elderly investors. FAC, ¶ 1.
- The payments the Vera Defendants received were the result of calls the Vera Defendants made "to defraud investors." FAC, ¶ 1.

- "Standing in the Receivership Entities' shoes for purposes of the claims asserted below and for the benefit of the Receivership Entities' defrauded creditors, including at least 1,300 elderly victims, the Receiver seeks to recover the funds fraudulently transferred to the [Vera Defendants]." FAC, ¶ 1.
- In the Receivership Order, the Court made a preliminary finding that the Receivership Defendants "have engaged and continue to engage in a fraudulent scheme to defraud at least 1,600 persons throughout the United States into purchasing gold and silver bullion" and that the Defendants "targeted a vulnerable population of mostly elderly or retirement-aged persons." FAC, ¶ 4.
- "As further described below, the [Vera Defendants] participated in this scheme by locating and contacting Investors and using fraudulent statements and omissions as described below, to lure investors into buying bullion and coins at grossly inflated prices." FAC, ¶ 5.
- "Each of the Receivership Entities existed and operated solely to perpetrate fraud on unsuspecting, vulnerable investors, and line the pockets of . . . the [Vera Defendants] they supervised." FAC, ¶ 50.
- "The Receivership Defendants used the [Vera Defendants] and made the transfers at issue in this lawsuit, to accomplish their goal. FAC, ¶ 51.
- "The [Vera Defendants] and each of them employed solicitations designed to instill fear in these elderly and retirement aged Investors FAC, ¶ 57.
- The Receiver alleges payments to each Broker Defendant was made by check, direct deposit, or wire transfer thus implicating the mail and wire fraud statutes. FAC, ¶ 97; see also FAC, Exhibit C-11 showing multiple payments made by check and wire to the Vera Defendants.

The Receiver's list of fraud-based allegations goes on further in the following paragraphs in the FAC: 64(a) – (e) (instilled fear), 65(a) – (d) (most egregious fraud), 67 (undisclosed and excessive markups), 69 (failed to disclose), 79 (false statements), 80 (false representations), 89 (state agencies investigating and issuing cease and desist letters), 92 (Barrick Capital and Receivership Defendants are a common enterprise), 95 (fraudulent sales), 101.f (fraudulent

transfers), 104.h (used Vera Defendants to sell bullion through false and misleading statements and practices), and 104.j (at the time of each transfer, the Receivership Entities was [sic] a fraudulent enterprise).

Any of these facts as alleged by the Receiver, if proven true, would form the basis for criminal liability under the Wire and Mail Fraud statutes. See 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1341 (Mail Fraud). This is especially so given the Receiver's listing of the payments made to the Vera Defendants by check and wire in Exhibit C-11 to the FAC.

As both parties have already briefed, the case for a stay is strongest when an indictment has already been returned. That is because, in the absence of an indictment, it is usually difficult for a Court to determine with certainty the degree of overlap between the criminal investigation and the allegations and/or causes of action asserted in the civil lawsuit. SEC v. AmeriFirst Funding, Inc., No. 3:07-CV-1188-D, 2008 WL 866065, at *3 (N.D. Tex. Mar. 17, 2008). However, here the Search Warrant removes any "speculation" about overlap the Receiver asserts in its Response may exist. Instead, the Court can see plainly the overlap between the criminal investigation and the allegations by the Receiver in the FAC, and can determine for itself the two matters have substantial, if not complete, overlap such that proceeding with the civil matter would infringe on the rights assured to the Vera Defendants' by the Fifth Amendment to the United States Constitution.

Therefore, the Vera Defendants request that this case be stayed until the conclusion of the pending criminal investigation.

Dated: March 11, 2025 Respectfully submitted,

/s/ Michael S. Alfred
Michael S. Alfred
State Bar No. 24014416
VerisLaw, PLLC
4843 Colleyville Blvd., Suite 251-391
Colleyville, Texas 76034
(817) 678-4121 telephone
(512) 717-7230 fax
malfred@verislaw.net

Counsel for Defendants Walter Vera, Verastan Group, LLC and Midwood Capital, LLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on March 11, 2025, I electronically filed the foregoing document with the clerk of court for the U.S. District Court, Northern District of Texas, Dallas Division, using the electronic case filing system, which sent a "Notice of Electronic Filing" to all attorneys of record, in accordance with the Federal Rules of Civil Procedure.

/s/ Michael S. Alfred
Michael S. Alfred

UNITED STATES DISTRICT COURT

for the Central District of California

In the Matter of the Search of)	CE
(Briefly describe the property to be searched or identify the person by name and address)) Case No. 2:20-MJ-04567	
8383 Wilshire Boulevard, Suite 700, 7th Floor, Beverly Hills, California 90211, as described in ATTACHMENT A))))	

CLER	FILED K, U.S. DISTR	
Sept	tember 2	3, 2020
CENTRAL BY:	DISTRICT O	F CALIFORNIA DEPUTY



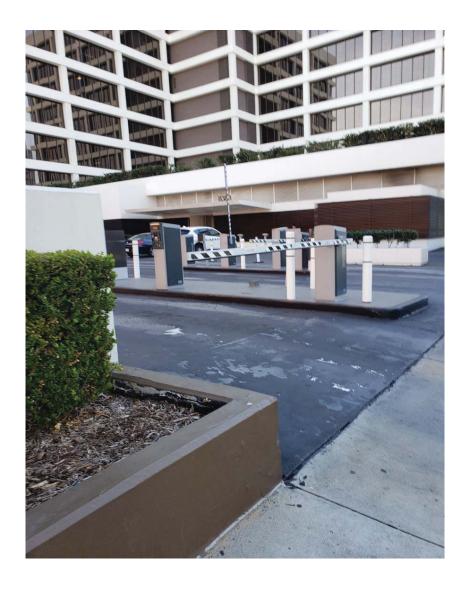
APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attornous penalty of perjury that I have reason to believe that on the property to be searched and give its location):	ey for the government, request a search warrant and state under ne following person or property (identify the person or describe the
See Attachment A	
located in the Central District of California, there is now	concealed (identify the person or describe the property to be seized):
See Attachment B	
The basis for the search under Fed. R. Crim. P.	41(c) is (check one or more):
☑ evidence of a crime;	
□ contraband, fruits of crime, or other item	ns illegally possessed;
property designed for use, intended for use	use, or used in committing a crime;
a person to be arrested or a person who	is unlawfully restrained.
The search is related to a violation of:	
Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1341	Mail Fraud
The application is based on these facts:	
See attached Affidavit	
□ Continued on the attached sheet.	
Delayed notice ofdays (give exact en under 18 U.S.C. § 3103a, the basis of which is set f	
	/s/ Kelly Luquette
	Applicant's signature
	Kelly Luquette, Special Agent, FBI Printed name and title
Attacted to by the applicant in accordance with the requirer	
Attested to by the applicant in accordance with the requirer	hents of Fed. R. Crini. P. 4.1 by telephone.
Date: September 23, 2020	
City and state: <u>Los Angeles, CA</u>	Michael R. Wilner

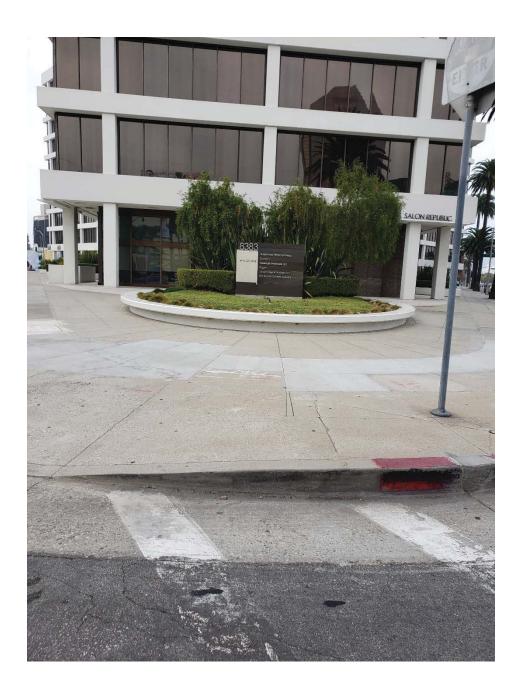
Printed name and title

ATTACHMENT A

The SUBJECT PREMISES is a business located at 8383 Wilshire Boulevard, Suite 700, 7th Floor, Beverly Hills, California, 90211, in the Los Angeles Division, Central District of California. The location is large white multi-floor commercial business building in which Metals.com and Tower Equity rent Suite 700. Outside Suite 700, there is a placard that reads, "Tower Equity." Images of the building follow:







ATTACHMENT B

I. ITEMS TO BE SEIZED

- 1. The items to be seized are evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), and/or 18 U.S.C. § 1956 and § 1957 (money laundering) (collectively the "Subject Offenses"), namely:
- a. Records relating to the identification of, marketing and advertising to, basis for selecting prospective customers, and/or efforts to retain current customers;
- b. Records relating to the purchase, sale, pricing, spreads or mark-ups on, refunds or rescissions, liquidation, and/or valuation of precious metals and/or real estate investments;
- c. Records relating to the selection of particular precious metals to be sold to customers;
- d. Records relating to SDIRA accounts, including completed, partially completed and blank application forms; the identities of Metals.com employees who facilitated completion of the application forms and rollovers; and any guidance and/or instructions provided to such employees regarding the completion of the application forms;
- e. Scripts used and/or to be used to sell precious metals and SDIRA accounts, including any exhibits and other supporting documents such as newspaper, magazine articles and/or

items available on the internet to be used in connection with the scripts;

- f. Lists of employees, aliases and false personal or background information used by employees, and all contact information for employees;
- g. Records of payroll, compensation, and/or commissions promised to and/or paid to any employee or principal of Metals.com and/or Tower Equity;
- h. Any faxes, emails, letters, SMS/Digital messages, recordings, or other correspondence between Metals.com employees and investors or customers regarding the value of precious metals, the performance and/or value of the investor or customers' portfolio, and/or any complaints and/or demands for refunds;
- i. Any faxes, emails, letters, SMS/Digital messages and/or other correspondence between Metals.com employees about the target customer market, sale of precious metals, pricing of precious metals, refunds or rescissions of sales of precious metals, the performance and/or value of investors' or customers' portfolios, and/or any complaints and/or demands for refunds;
- j. Records relating to the "tuck in" and other responses to investors and customers who questioned the value of their purchase after its completion, whether in written or verbal form, including the identities of the individuals who created, directed, or provided written or verbal "tuck ins" to customers;

- k. All recordings of conversations between
 Metals.com employees and investors, including deleted or edited recordings;
- Records relating to investments in real estate by Metals.com or Tower Equity;
- m. Checks or copies of checks received from customers and/or dispersed to customers;
- n. Records of customers' payments to Metals.com and Tower Equity and outgoing transfers or uses of those funds;
- o. Records of all payments for precious metals made by or received by Tower Equity or Metals.com;
- p. Records of Metals.com's and Tower Equity's payments to and payments received from Bayside Metals Exchange and Dillon Gage, including records disclosing the purpose of the payment;
- q. Financial records and bank records pertaining to Tower Equity or Metals.com or any of those businesses' customers/clients from on or about January 2016 to the present;
- r. Records demonstrating collectability, numismatic or semi-numismatic value of any version of the polar bear coin marketed or sold by Metals.com;
- s. Any records that show the identity, address, social security number, phone number, or any other personal and/or financial data demonstrating control over the SUBJECT PREMISES and/or Metals.com and/or Tower Equity;

- t. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
- i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
- ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - iii. evidence of the attachment of other devices;
- iv. evidence of counter-forensic programs (and
 associated data) that are designed to eliminate data from the
 device;
 - v. evidence of the times the device was used;
- vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

- 2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.
- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

4. As used herein, the term "Metals.com" includes any prior or successor entity, including all of the following:
Chase Metals, LLC; Chase Metals, Inc.; TEM, Inc.; TMTE, Inc.;
Metals.com; Barrick Capital or barrickcapital.com, and USA Mint.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

- 5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:
- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.
- b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.
- i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine

whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

- ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.
- c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.
- d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.
- e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.
- f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may

retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

- g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.
- h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.
- 6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

 Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.
- 7. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.